COOLEY LLP
JEFFREY M. GUTKIN (216083)
(jgutkin@cooley.com)
AARTI REDDY (274889)
(areddy@cooley.com)
AMY M. SMITH (287813)
(amsmith@cooley.com)
MORGAN LEWIS (322205)
(melewis@cooley.com)
JULIA M. IRWIN (352861)
(JIrwin@cooley.com)
3 Embarcadero Center, 20th Floor
San Francisco, California 94111-4004
Telephone: +1 415 693 2000
Facsimile: +1 415 693 2222

COOLEY LLP
JORGE L. SARMIENTO (*Pro Hac Vice*)
(jsarmiento@cooley.com)
55 Hudson Yards
New York, NY 10001-2157
Telephone: +1 212 479 6000
Facsimile: +1 212 479 6275

Attorneys for Defendant
LINKEDIN CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

V.R. individually and on behalf of all others similarly situated,

Plaintiff,

v.

LINKEDIN CORPORATION,

Defendant.

Case No. 5:24-CV-07399-PCP

DEFENDANT LINKEDIN CORPORATION'S NOTICE OF MOTION AND MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF MOTION TO DISMISS PLAINTIFF V.R.'S COMPLAINT

Date: March 6, 2025
Time: 9:00 a.m.
Dept: Courtroom 4, 5th Fl.
Judge: Edward J. Davila
Trial Date: TBD
Date Action Filed: October 23, 2024

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

TO THE COURT, ALL PARTIES AND TO THEIR ATTORNEYS:

Please take notice that on March 6, 2025 at 9 a.m. in Courtroom 4 of the above-captioned court, located at 280 South 1st Street, San Jose, California 95113, or as soon thereafter as the matter may be heard, defendant LinkedIn Corporation ("LinkedIn") will, and hereby does, move this Court for an order under Federal Rule of Civil Procedure 12(b)(6), dismissing the Complaint filed in this action by plaintiff V.R. against LinkedIn in their entirety, with prejudice.

ISSUES TO BE DECIDED

Whether the Court should dismiss Plaintiff's California Invasion of Privacy ("CIPA") § 631 and § 632 and California constitutional claims in the Complaint ("Complaint") because she has failed to state a claim under Rule 12(b)(6).

MEMORANDUM AND POINTS OF AUTHORITIES

I. INTRODUCTION

This lawsuit is Plaintiff's counsel's ***fifth*** attempt to assert pixel claims against defendant LinkedIn, Inc ("LinkedIn"). Plaintiff V.R. claims that when she and class members visited certain webpages on CityMD's website to browse for information about a potential hospital visit, information about her interactions with that website was transmitted to LinkedIn. LinkedIn offers its advertisers the option to install a web pixel or "Insight Tag" (in LinkedIn's parlance) to aid their advertising efforts. According to Plaintiff, because CityMD allegedly installed the Insight Tag on certain webpages, LinkedIn should be held liable under California's Invasion of Privacy Act ("CIPA") and for invasion of privacy under the California Constitution. Plaintiff's claims —which are supported by allegations her counsel has essentially copy-pasted from their other actions—are meritless and should be dismissed with prejudice.

As an initial and dispositive matter, both of Plaintiff's CIPA claims fail because—as a New York Plaintiff visiting a non-California website—she has not sufficiently pled that California law applies to her claims. Even setting that defect aside, her claims fail for a host of other reasons.

Section 631. Plaintiff alleges that LinkedIn violated the first three clauses of the statute, because LinkedIn "intentionally taps, or makes any unauthorized connection . . . with any telegraph or telephone wire, line, cable or instrument," (clause one), willfully intercepted Plaintiff's

communications with CityMD and read, attempted to read, or learned their contents (clause two) and used their contents (clause three). *See* Cal. Penal Code § 631. Each claim fails. ***First***, nothing in Plaintiff's pleading alleges that LinkedIn acted as anything more than a ***vendor*** of an advertising tool that received information for CityMD's benefit. Accordingly, LinkedIn is a party to the communication that has no liability. ***Second***, Plaintiff's CIPA clause-one claim also fails because, as courts have uniformly held, such a claim is not cognizable as to internet communications. ***Third***, Plaintiff also failed to make any factually supported allegation or, in some cases any allegation at all, regarding several elements of her clause-two claim. Plaintiff did not sufficiently allege that LinkedIn read or attempted to read these alleged CityMD communications, that it intercepted them "in transit," that LinkedIn acted willfully, or that the alleged communications were "received" in California. ***Lastly***, Plaintiff's CIPA clause-three claim also fails because it rests on the flawed clause-one and clause-two claims. The Court should dismiss this claim with prejudice.

Section 632. Plaintiff's claim under Section 632 of CIPA fares no better. To survive dismissal, Plaintiff must allege that LinkedIn intentionally recorded a "confidential" communication by means of an "amplifying or recording device." *See* Cal. Penal Code § 632. Nothing in her pleading plausibly avers that LinkedIn acted with the requisite intent—indeed, her allegations regarding LinkedIn's state of mind largely parrot CIPA's statutory language. Further, as many courts have held, software code like the Insight Tag is not a "device" under the statute. Plaintiff also does not plausibly allege that her alleged communications were "confidential," as it is well settled that internet communications are presumptively ***not*** so.

Finally, neither of Plaintiff's CIPA claims can survive dismissal because she does not plausibly allege that the underlying data purportedly transmitted to LinkedIn via the Insight Tag qualifies as a "communication" under statute.

Invasion of Privacy. Plaintiff does not adequately plead a violation of California's constitutional right to privacy. The claim fails both because it is premised on her defective wiretapping claim, and because Plaintiff can allege no protected privacy interest in unspecific logistical information never used. Nor can Plaintiff allege a reasonable expectation of privacy in information that she voluntarily input on CityMD's website after being fully apprised that LinkedIn

may receive information about her interactions with other websites. Finally, Plaintiff cannot clear the high bar for alleging a "highly offensive" intrusion sufficient to support a constitutional claim.

For all of these reasons, the Complaint should be dismissed with prejudice.

II. BACKGROUND

A. The Parties

LinkedIn is a Delaware corporation headquartered in Sunnyvale, California. The company has created "the world's largest professional network on the internet," which provides a valuable "tool to help users find jobs or expand their professional network." (Compl. ¶ 17.) Plaintiff V.R. alleges she resides in New York and claims to have "maintained an active LinkedIn account at all relevant times." *(Id.* ¶ 7.) Plaintiff alleges that when she "created her LinkedIn account she agreed to LinkedIn's User Agreement," (*id.*), and that "[w]hen first signing up . . . users agree to . . . [LinkedIn's] Privacy Policy and [] Cookie Policy." (*Id.* ¶ 32.) Plaintiff does not allege that CityMD has any ties to California, and public records establish that VillageMD, the entity that owns and operates CityMD's website, resides in New Jersey. (*Id.* ¶ 1; Declaration of Aarti Reddy in Supp. Def. LinkedIn Corp. Mot. to Dismiss ("Reddy Decl.") Ex. E.)

B. LinkedIn's Insight Tag

LinkedIn enables advertisers to run advertising campaigns. (Compl. ¶¶ 17-18.) Through its Marketing Solutions services, advertisers can target advertisements based on audience characteristics. (*Id.* ¶ 18.) LinkedIn's Insight Tag is a piece of JavaScript code that advertisers can install on their websites to enable features like campaign reporting to facilitate advertising and marketing campaigns. (*Id.* ¶¶ 24-25; *see also* Reddy Decl. Ex. A.) When a LinkedIn member visits a website where an advertiser installed a tag, the member's browser sends certain information about that visit to LinkedIn, (Compl. ¶¶ 26-28), some of which is then allegedly sent to LinkedIn's Marketing Solutions advertising systems, where it is provided to advertisers to optimize their advertising campaigns, facilitate advertising retargeting, or learn more about their audiences. (*Id.* ¶¶ 18-20.) By helping advertisers analyze their website visitor information, LinkedIn enables those advertisers to target their advertisements to the most receptive LinkedIn members. (*Id.* ¶¶ 21-22.) Notably, while Plaintiff contends that LinkedIn "obtain[s]" "personal information and

communications" (*id.* ¶ 20) to help advertisers "target . . . account holders for advertising" (*id.* ¶ 30), nowhere does she plausibly allege that LinkedIn uses any such data for its own purposes.

C. CityMD's Use of LinkedIn's Insight Tag

Plaintiff alleges that "CityMD is a provider of accessible healthcare services that permits patients to schedule appointments at their brick-and-mortar locations through its Website." (*Id.* at ¶ 38.) According to Plaintiff, CityMD installed the Insight Tag on pages through which users booked appointments. (*See id.* ¶¶ 40-41.) Plaintiff further alleges that as a LinkedIn member books an appointment on the CityMD website, the Insight Tag on its pages sends various information to LinkedIn, including the person's appointment time and reason for the booking, and a cookie identifier for the member. (*Id.* ¶¶ 41-44.) Notably, Plaintiff does not allege that the Insight Tag is installed on any CityMD patient portal that would collect sensitive, medical information.

Plaintiff contends that, while booking an appointment, her activity on CityMD's website was transmitted to LinkedIn via the Insight Tag and that at the time, she was not aware that CityMD had installed the Insight Tag on its website. (*Id.* ¶ 8.) Plaintiff does not identify any specific information she purportedly transmitted to CityMD, nor does she contend that she received targeted advertising from either CityMD or LinkedIn or that LinkedIn actually used ***her*** data in any way.

III. ARGUMENT

A. California's Choice-of-Law Rules Bar Plaintiff's Section 631 and 632 Claims.

First, all of Plaintiff's CIPA claims fail because she has not pled that her claims are tied to California. California's choice-of-law rules provide that "the class action proponent bears the initial burden to show that California has 'significant contact or significant aggregation of contacts' to the claims of each class member." *Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 589 (9th Cir. 2012). Applied here, Plaintiff has not made a threshold showing that either she or the putative class—which encompasses "all LinkedIn account holders in the United States who booked a medical appointment" on CityMD's website—has the requisite ties to California. (Compl. ¶ 48.) This is particularly so because CityMD has no alleged ties to California. (Reddy Decl. Ex. E).

Even if Plaintiff had established these threshold contacts, and she has not, the Court would proceed to apply California's government interests test to determine whether California law

displaces the interests of other states. That test considers (1) whether the laws of the relevant jurisdiction differ; (2) whether those differences are material; and (3) if yes, which state has a greater interest in application of its laws. *Mazza*, 666 F.3d at 589-90.

The first two prongs of this test are easily satisfied, as "[t]here are material differences between CIPA and the wiretapping statutes of the other 49 states." *In re Yahoo Mail Litig.*, 308 F.R.D. 577, 602 (N.D. Cal. 2015) (finding nation-wide class could not bring CIPA claims); *Doe v. Kaiser Found. Plan, Inc.*, 2024 WL 1589982, at *12 (N.D. Cal. Apr. 11, 2024 (same); *James v. Walt Disney Co.*, 701 F. Supp. 3d 942, 964 (N.D. Cal. 2023) (same). This is true of New York law, which requires only single party consent. *Compare People v. Badalamenti*, 27 N.Y.3d 423, 432 (2016) (stating New York requires one party consent) *with* §§ 631-632 (requiring dual consent).

As to the third prong, "'each foreign state has an interest in applying its law to transactions within its borders,' which means that 'if California law were applied to [a nationwide class], foreign states would be impaired in their ability to calibrate liability to foster commerce.'" *Yahoo Mail Litig.*, 308 F.R.D. at 603 (quoting *Mazza*, 666 F.3d at 593) (finding "California's interest in applying its law to nonresidents who send or receive emails from Yahoo Mail subscribers in other states . . . attenuated"). The language of CIPA itself confirms this interpretation, because it explicitly limits its application to protecting persons within the state. *Id.* ("in enacting CIPA, the California legislature specifically stated that its intent was to 'protect the right of privacy of the *people of this state*.") (quoting Cal. Penal Code § 630) (collecting other authority). Most recently, in *Kaiser*, the court dismissed the CIPA claims of plaintiffs outside California even though the defendant (Kaiser) resided in California. The Court found that plaintiffs' respective home-states had a more significant interest in application of their wiretap laws. *Kaiser*, 2024 WL 1589982, at *13 ("the wiretapping law that applies turns on the residence of the Kaiser plan member."). That reasoning applies here. As the *Kaiser* court aptly held, "[b]ecause wiretapping statutes are designed to protect the privacy interests of individual members, the residences of the individuals are more important to the respective sovereign than the residence of the alleged wrongdoer." *Id.* Accordingly, as Plaintiff is a New York resident, New York law should apply to her claims.

Finally, LinkedIn anticipates that Plaintiff may try to invoke the California choice-of-law

clause in LinkedIn's User Agreement to circumvent CIPA's territoriality requirement. (Compl. ¶ 7; 58). The Court in *Doe v. Kaiser* rejected this exact argument. 2024 WL 1589982, at *11-12. There, the Plaintiff sought to apply CIPA based on a California choice-of-law clause in defendant Kaiser's terms of use. The Court was unmoved, explaining that the Ninth Circuit has "recognized that parties' agreement to apply California law must yield to those circumstances where the law in question contains 'geographical limitations'" and that "CIPA does contain express geographical limitations." *Id.* (quoting *Gravquick A/S v. Trimble Navigation Int'l*, 323 F.3d 1219, 1223 (9th Cir. 2003)); *see also* § 630 ("The Legislature by this chapter intends to protect the right of privacy of the people of this state."); § 631(a) (limiting law to communications moving "within this state"). It thus concluded that the choice-of-law provision in Kaiser's TOU "has no force." *Kaiser*, 2024 WL 1589982, at *12. Here too, the User Agreement's choice-of-law clause cannot save Plaintiff's CIPA claims.

B. Plaintiff Fails to State a Claim Under CIPA § 631 For Other Reasons.

Even if the Court were to allow Plaintiff's CIPA claims to proceed, her Section 631 claims would still fail. Plaintiff asserts claims under the statute's first three clauses. (Compl. ¶¶ 60-72.) Clause-one applies to any person who intentionally tapped, electrically or otherwise, Plaintiff's transmissions. Cal. Penal Code § 631(a). Section 631's second clause applies to "[a]ny person . . . who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any . . . communication while the same is in transit . . . within this state." *Id*. Its third clause applies to any person "who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information" obtained in violation of these other clauses. *Id*. Each claim fails for multiple reasons.

First, each of Plaintiff's Section 631 claims are barred by the party exception. As a vendor that provided a tool to assist CityMD with its marketing and advertising efforts, LinkedIn was a party to Plaintiff's alleged communications with CityMD, not a third-party "eavesdropper." ***Second***, Plaintiff fails to plead violation of CIPA's clause-one because it only "concerns telephonic wiretapping specifically" and "does not apply to the context of the internet." *Williams v. What If Holdings, LLC*, 2022 WL 17869275, at *2 (N.D. Cal. Dec. 22, 2022). ***Third***, Plaintiff also fails to

plausibly allege many of the requisite elements of her claim under CIPA's second clause, including that (1) LinkedIn "read or attempted to read, or to learn the contents or meaning of" any purported communication, (2) that any alleged interception occurred while the communication was "in transit," (3) "within this state" and that (4) any such interception was "willful." Cal. Penal Code § 631(a). ***Finally***, Plaintiff does not state a claim under CIPA's third clause because this claim is entirely derivative of her deficient clause-one and clause-two claims, and because she has not plausibly pled that LinkedIn "use[d] or attempted to use" the challenged information. *Id.*

1. LinkedIn Is Not Liable Under CIPA Section 631 Because It Was a Party to the Alleged Communications, Not a Third-Party Eavesdropper.

To begin, all of Plaintiff's Section 631 claims fail under CIPA's party exception. It is well established that CIPA applies "only to eavesdropping by a third-party and not to recording by a participant to a conversation." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 607 (9th Cir. 2020) (quoting *Warden v. Kahn*, 99 Cal. App. 3d 805, 811 (1979)). Plaintiff's bare pleading fails to allege that LinkedIn acted as anything more than an extension of and a service provider to CityMD, which was a party to the alleged communications. The leading case on this topic, *Graham v. Noom, Inc.*, analyzed a similar theory and held that a third-party vendor did not violate CIPA where it merely "provide[d] a software service that captures its clients' data . . . and allow[ed] the clients to analyze their data" but had not "intercepted and used the data itself." 533 F. Supp. 3d 823, 832 (N.D. Cal. 2021). Rather, the vendor operated as "an extension of Noom," the website operator, offering "a tool . . . that allows ***Noom*** to record and analyze ***its own data*****[.]**" *Id.* (emphases added). Numerous courts across this district have endorsed this reasoning. *See, e.g.*, *Love v. Ladder Fin., Inc.*, 2024 WL 2104497, at *1 (N.D. Cal. May 8, 2024) (finding *Graham* analysis dispositive of CIPA claims); *Doe I v. Google LLC*, 2024 WL 3490744, at *6 (N.D. Cal. July 22, 2024) (applying Graham); *Williams*, 2022 WL 17869275, at *3.[1]

[1] *See also, e.g.*, *Yale v. Clicktale, Inc.*, 2021 WL 1428400, at *1, *3 (N.D. Cal. Apr. 15, 2021) (vendor providing "Event Triggered Recorder" software was not a third-party eavesdropper since it "allows its clients to monitor their website traffic"); *Johnson v. Blue Nile, Inc.*, 2021 WL

The same analysis necessitates dismissal here. Plaintiff has not pled that LinkedIn acted as anything more than an extension of CityMD. Indeed, both her pleading and documents incorporated by reference in the Complaint establish that the Insight Tag is ***installed by website owners.*** (*See* Compl. n.17 (citing LinkedIn's "Insight Tag" webpage (attached as Reddy Decl. Ex. A) which describes how advertisers can "manually install the tag . . . yourself[.]") (emphasis added); *see also* Compl. ¶ 25 (explaining that the "Insight Tag is a JavaScript-based code which allows for the installation of its software").) She plainly alleges LinkedIn represents to its customer advertisers that the tag is "[a] simple code snippet added to [a] website [that] can ***help you*** optimize ***your campaigns***, retarget ***your website visitors***, and learn more about ***your audiences***." (Compl. ¶ 24 (emphasis added).) Her allegations—which are near-verbatim copied from her counsel's other complaints—then focus on how these tools "***allow[] marketers*** . . . to target potential customers"; "***allow advertisers*** to select specific characteristics to help them reach their ideal audience"; and "***allow potential advertisers*** to '[b]uild strategic campaigns.'" (*Id*. ¶¶ 18, 21 (emphasis added).) Nowhere does Plaintiff allege that LinkedIn shared any CityMD data (let alone her data) with other advertisers or that it used such data for any independent purpose. At most, Plaintiff contends that the Insight Tag generally sends certain cookies that allow LinkedIn to identify the user associated with certain Insight Tag transmissions, and then offers a conclusory assertion (again, copied from other pleadings) that LinkedIn can use this information to target ads to account holders. (Compl. ¶ 30.) This bald allegation is not supported by any well-pled facts, and in fact, it is contradicted by the other allegations demonstrating that LinkedIn merely provides data to advertising customers regarding ***their own*** website visitors to facilitate ***their own*** ad campaigns. (*See, e.g.*, Compl. ¶¶ 18-22, 24.) Accordingly, the Complaint alleges only that LinkedIn collected and maintained information received ***at the direction*** of CityMD, to enable advertising requested ***by*** CityMD. Just as in *Graham*, *Love*, *Williams*, and other cases, Plaintiff has failed to allege that LinkedIn's Insight Tag was anything more than a mere "tool that [defendant] used to record its own communications with plaintiff." *Williams*, 2022 WL 17869275, at *3; *see also Love*, 2024 WL 2104497, at *1

1312771, at *1 (N.D. Cal. Apr. 8, 2021) (similar).

("[P]laintiffs have only alleged that FullStory provides a tool that allows Ladder to record, track, and analyze the interactions that users have with its own site.").

For many courts, the analysis begins and ends with *Graham*. Plaintiff may, however, invoke another line of cases holding that an analytics provider is not an extension of a defendant if it has "the capability to use" communications for any other purpose than supporting the website operator. *Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023). Even if the Court adopted the *Javier* framework, Plaintiff's claims would still fail because she has not alleged that LinkedIn is capable of using information received from CityMD for LinkedIn's own independent purposes.

As explained above, rather than alleging capability of use, Plaintiff's allegations focus on how the Insight Tag "allows marketers and advertisers" to conduct targeted advertising. (Compl. ¶ 21.) At most, Plaintiff generally asserts that "LinkedIn incorporated the information it intercepted from the CityMD's Website" into unspecified "marketing tools to fuel its targeted advertising service." (*Id*. ¶ 45; *see also id.* ¶ 20 ("personal information and communications obtained by LinkedIn are used to fuel various services offered via LinkedIn's Marketing Solutions").) She further alleges that the Insight Tag may transmit certain cookies that enable LinkedIn to identify members and that based on this data, LinkedIn is "able to" target its own members with ads. (*Id*. ¶¶ 25-29.) Nowhere does she elaborate on these bare allegations, let alone allege that she ever saw or received targeted ads herself, that any other specific LinkedIn member did, or that LinkedIn targeted ads based on her or anyone else's Insight Tag data for any customer other than CityMD.

As court after court applying *Javier* has held, a plaintiff must plead ***specific facts*** to support an inference that a vendor independently used the underlying communication. For example, in *Heiting v. Athenahealth, Inc.*, 2024 WL 3761294, at *4 (C.D. Cal. July 29, 2024), allegations that Salesforce "may record, store, and use" the underlying data and "uses chat data to enhance its own business" were "too general and conclusory to support a reasonable inference that Salesforce had the capability to use the communications for any purpose beyond providing it to Defendant." *Id* (dismissing case). These are akin to Plaintiff's allegations here that LinkedIn uses the challenged data to "fuel various services." (Compl. ¶ 20.) Multiple courts have likewise dismissed CIPA claims based on similarly vague allegations. *See, e.g.*, *Valenzuela v. Super Bright LEDs Inc.*, 2023 WL

8424472, at *8 (C.D. Cal. Nov. 27, 2023) (finding plaintiff's allegation that chat vendor had "capability to use its record of [w]ebsite users' interaction[s]" for data analytics and marketing/advertising to consumers "conclusory and insufficient"); *Swarts v. Home Depot, Inc.*, 689 F. Supp. 3d 732, 737-38, 745 (N.D. Cal. 2023) (allegations that defendant "analyz[ed] the data and provid[ed] [] customer data metrics related to each conversation" and "accesse[d] and analyze[d]" those "conversations" were not sufficient to show capability of use); *Yockey v. Salesforce, Inc.*, 688 F. Supp. 3d 962, 973 (N.D. Cal. 2023) (dismissing CIPA claim that the provider "analyzes the customer-support agent interactions in real time to create live transcripts of communications"). By contrast, those courts that have denied dismissal based on *Javier* have done so based on allegations that are far more robust than those pled by Plaintiff. *See, e.g.*, *Yockey v. Salesforce, Inc.*, 2024 WL 3875785, at *4 (N.D. Cal. Aug. 16, 2024) (finding capability of personal use where plaintiff alleged Salesforce fed chat communications into its "data intelligence platform" to "train the AI models that form the basis of some of [Salesforce's] services"); *Jones v. Peloton Interactive, Inc.*, 2024 WL 3315989, at *4 (S.D. Cal. July 5, 2024) (capability of personal use adequately alleged where plaintiff alleged that "Drift analyzes and uses the chat conversations it intercepts [to improve its machine learning technologies] all of which *independently benefits and serves*" Drift).

LinkedIn acknowledges that Judge Pitts denied a motion to dismiss involving LinkedIn's Insight Tag. LinkedIn respectfully submits that this decision was in error. The Court dispensed with the vendor argument without rigorous analysis and concluded that the plaintiff in *Jackson* plausibly alleged independent use based on only a few general allegations that the defendant "monetizes the collected data through the sale of ads" and "enables advertisers to target users with relevant content[.]" *Jackson v. LinkedIn Corp.*, 2024 WL 3823806, at *5 (N.D. Cal. Aug. 13, 2024). But, as many courts facing similar facts have held, such conclusory allegations are not enough to plead that LinkedIn used data independently, as an eavesdropper. Here, the Court should not follow *Jackson*'s lead and should instead dismiss Plaintiff's CIPA claims because she has not alleged, even in a conclusory fashion, that LinkedIn has the capability to use her alleged communications for its own purposes, let alone made those allegations with the required specificity.

Finally, even if the Court found Plaintiff's sparse allegations regarding LinkedIn's advertising services sufficient to plead capability of use under *Javier*, her claims would still fail for an independent reason. None of her allegations regarding the analytics tool at issue (Insight Tag) are ***tethered to CityMD***, let alone Plaintiff's specific communications with CityMD's website. In *Cody v. Ring LLC*, the Court found allegations of use "conclusory" where they were based on public reporting that the analytics provider "exploited" chat data for "targeted advertising" but said "nothing about ***Ring*** [defendant website] or about Meta or Kustomer using ***Ring*** data to create targeted advertising." 718 F. Supp. 3d 993, 1003 n.3 (N.D. Cal. 2024) (emphasis added); *see also Doe I*, 2024 WL 3490744, at *3 (dismissing CIPA claims where the complaint "relie[d] heavily on Google's own product descriptions" and lacked allegations as to the use of Google Analytics by the healthcare websites at issue). The same defect plagues Plaintiff's complaint. She relies on generic descriptions regarding "the various services offered via LinkedIn Marketing Solutions," and does not adequately allege facts connecting the Insight Tag to the challenged website. (Compl. ¶ 20.) Such allegations are not sufficient to state a claim under any of Section 631's clauses.

2. Plaintiff's Clause-One Claim Fails for Additional Reasons.

Plaintiff cannot assert a clause-one claim because this provision "prohibits telephonic wiretapping, which does not apply to the internet." *St. Aubin v. Carbon Health*, 2024 WL 4369675, at *4 (N.D. Cal. Oct. 1, 2024) (citation omitted); *Ramos v. Gap Inc.*, 2024 WL 4351868, at *3 (N.D. Cal. Sept. 30, 2024) (collecting cases). Plaintiff alleges only internet transmissions, and her clause-one claim fails. (Compl. ¶ 64.)

3. Plaintiff's Claim Under CIPA's Second Clause Has Additional Defects.

Plaintiff's clause-two claim also fails because she has not pled that LinkedIn: (1) "read or attempted to read" her "communications," (2) while they were "in transit," (3) within the state, nor that it (4) did so "willfully." Cal. Penal Code § 631(a). Each of these failures is dispositive.

Read or Attempting to Read. Under CIPA's second clause, Plaintiff must at least plausibly allege facts concerning LinkedIn's attempt to "read, or to learn the contents" of any purported communications. *Id.* Plaintiff's conclusory allegation that LinkedIn read or attempted to "read, or learn the contents or meaning of Plaintiff's and Class Members' communications to CityMD" is a

mere recitation of the claim's elements and is not entitled to a presumption of truth. (Compl. ¶ 68; *see also id.* ¶ 65); *see Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). At most, Plaintiff alleges that LinkedIn ***received*** her alleged communications, not that it read or attempted to learn their contents. (*See* Compl. ¶ 36 (explaining only how "LinkedIn . . . ***intercepts and receives***" the challenged information) (emphasis added).) In *James v. Allstate Insurance Company*, for example, the plaintiff alleged that the defendant's analytics provider "recorded the data and store[d] it on its servers." 2023 WL 8879246, at *3 (N.D. Cal. Dec. 22, 2023). The court found such allegations "insufficient to support a plausible interference [that] [the analytics provider] attempted to read or learn the contents of the communications while in transit." *Id.* Plaintiff's allegations that LinkedIn "obtained" certain data from CityMD are similarly deficient. (Compl. ¶ 20.) As in *James*, Plaintiff has not pled any facts creating a plausible inference that LinkedIn read or attempted to learn the contents of her alleged communications with CityMD, such as by alleging that she was served ads related to information she shared with CityMD. *See Love*, 2024 WL 2104497, at *2 (finding allegation that defendant "may use and share information in an aggregated and de-identified manner" insufficient as it created "no coherent story of how or why FullStory would learn such granular information about users of one of its customers' sites").

Further, an analytics provider that offers a tool to allow customers to process their own data cannot be said to read or learn the contents of a communication. (*See* Compl. ¶ 24.) If that amounted to a CIPA violation, every software-as-a-service provider would be liable for the use of their tool on any website. Such ubiquitous practices cannot violate CIPA or fit within *Ribas v. Clark*, 38 Cal. 3d 355 (1985), the California Supreme Court's long-standing decision regarding whether a third party is an extension of a party to the communication.

In Transit. "[T]he crucial question under § 631(a)'s second clause is whether [plaintiff] has plausibly alleged that [defendant] read one of his communications while it was still in transit, i.e., before it reached its intended recipient." *Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1137 (E.D. Cal. 2021); Cal. Penal Code § 631(a). This means that to state a claim under CIPA's second clause, the plaintiff must allege specific facts including "***when*** the interception occurs." *Swarts*, 689 F. Supp. 3d at 746 (emphasis added). "While Plaintiff[] need not prove [his] theory of interception on

a motion to dismiss, Plaintiff[] must provide fair notice to Defendant[] of when [he] believe[s] [Defendant] intercepts [his] communications." *In re Vizio Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1228 (C.D. Cal. 2017); *see also Esparza v. Gen Digit. Inc.*, 2024 WL 655986, at *4 (C.D. Cal. Jan. 16, 2024) (emphasis added) (dismissing CIPA claims involving pixel technology where "Plaintiff fail[ed] to allege specific facts about . . . when the interception took place, and how the interception took place").[2] Merely parroting the terms of the statute by baldly alleging the interception occurs "in transit," (Compl. ¶ 68), Plaintiff pleads no facts to support her allegation, nor does she describe when the alleged interception takes place. Her claim fails for this reason as well.

Sent or received within California. As another Court in this district recently recognized, Section 631 "contain[s] express geographical limitations." *Kaiser*2024 WL 1589982, at *12. The statute itself provides that the defendant must intercept the plaintiff's "communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received ***at any place within this state***." *Id.* (quoting § 631). To plead a CIPA claim, the Plaintiff must therefore allege she was sending or receiving a message from within California. Plaintiff—who is a New York resident—does not even allege she has ever ***been*** to California, let alone sought to schedule a medical appointment there. (Compl. ¶ 7.) She further alleges that she was communicating with CityMD, which has no apparent ties to California. Ex. E. In short, nothing she pleads suggest that either she or CityMD have any ties to California. This too is dispositive.

Willful. To state a clause-two claim, Plaintiff must plausibly allege LinkedIn "willfully" obtained and read, or attempted to read, her communications with CityMD. Here too, Plaintiff's allegations are little more than a bare recitation of elements copied from her counsel's other

---

[2] *Cody*, 718 F. Supp. 3d at 1001 (dismissing and finding allegation that "application program is 'plugged into' Ring's website and allows chats to be routed 'in real time' . . . fail[s] to provide specific factual allegations"); *Rodriguez v. Google LLC*, 2022 WL 214552, at *2 (N.D. Cal. Jan. 25, 2022) ("Using the word 'intercept' repeatedly is simply not enough" to "make it plausible Google is intercepting [plaintiff's] data in transit").

pleadings, they are thus not entitled to a presumption of truth. *Twombly*, 550 U.S. at 570. She pleads that "LinkedIn, willfully and without the consent of Plaintiff and Class Members, read or attempted to read, or learn the contents or meaning of Plaintiff's and Class Members'" and "used or attempted to use the communications and information they received through their tracking technology, including to supply advertising services." (Compl. ¶¶ 68-69.) Without citing any factual basis, Plaintiff asserts that "LinkedIn intends to intercept this protected and sensitive health data due to the value" and that "LinkedIn is well aware of the dangers of incorporating such technology on websites that offer medical and health services, but continues to do so." (*Id.* ¶ 9.) But Plaintiff pleads no facts to render these allegations plausible, and must do more to state a violation of CIPA. Courts dismiss similar claims based on far more detailed allegations of intent. *Cf. Heiting v. Taro Pharms. USA, Inc.*, 709 F. Supp. 3d 1007, 1019 (C.D. Cal. 2023) (holding allegations that "Defendant paid Genesys to intercept messages . . . [did not] demonstrat[e] Defendant acted with the requisite knowledge or intent to aid and abet Genesys's purported CIPA violation"). Even if such allegations were sufficient, Plaintiff cannot plausibly allege intent on the face of LinkedIn's policies disclosing the ***opposite*** intention—that LinkedIn does not want to receive sensitive information and expressly prohibits websites from transmitting such data to LinkedIn through its Advertising Agreement and Ads Policies. (Reddy Decl. Ex. B, LinkedIn Ads Agreement ("You will also not transfer to LinkedIn any data that . . . constitutes Sensitive Data, including by way of installing the Insight Tag on a page that collects medical, financial, or other Sensitive Data about identified or identifiable individuals."); *id.* Ex. C, LinkedIn Advertising Policies) ("Ads must not target based on sensitive data or categories . . . including medical information and consumer health data.").) Stated simply: "There is nothing inherently unlawful about [LinkedIn] offering its source code" to CityMD—"at least [given LinkedIn's] admonitions" to CityMD that it "must avoid transmitting" health, medical, or other sensitive data. *Doe I*, 2024 WL 3490744, at *4.

Doe's reasoning is apt. There, Judge Chhabria found "plaintiffs have not adequately alleged that Google intentionally obtained patients' private health information" via Google Analytics, *inter alia*, because "Google repeatedly told developers not to send personally identifiable information" and thus "purposefully acted so as ***not*** to receive any personal health information." *Id.* Plaintiff's

claim here fails under the same reasoning.

4. Plaintiff's Claim Under CIPA's Third Clause Has Further Flaws.

To plead a valid clause three claim, a Plaintiff must allege a "a violation of the first or second clauses." *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 827 (N.D. Cal. 2020). As "Plaintiff[] ha[s] not done so, [she] ha[s] failed to plead a violation of third clause[.]" *Id.*

Additionally, as discussed above, Plaintiff pleads no facts that render plausible her allegation that LinkedIn independently used any of the allegedly intercepted information. Her conclusory allegation that LinkedIn "is able to target its account holders for advertising" alleges what is possible, but not what occurred here. (Compl. ¶ 30.) And her claim that "personal information and communications obtained by LinkedIn are used to fuel various services offered via LinkedIn's Marketing Solutions" is inadequate to plead that LinkedIn used any of her data. (*Id.* ¶ 20.) These general allegations are simply not tethered to CityMD or Plaintiff. In this way, this is an even more attenuated series of allegations than those rejected in *James*: that "record[ing] the data and stor[ing] it . . . is insufficient to support a plausible interference [*sic*] [the analytics provider] attempted to read or learn [its] contents[.]" 2023 WL 8879246, at *3.

C. Plaintiff Fails to State a Claim Under CIPA § 632.

To state a Section 632 claim, Plaintiff must show, *inter alia*, that LinkedIn intentionally recorded a confidential communication by means of an "amplifying or recording device." *See* Cal. Penal Code § 632. Plaintiff has not satisfied her pleading burden because she fails to adequately allege that LinkedIn "intentionally" recorded a "confidential" communication, and that the Insight Tag—a piece of JavaScript software code—qualifies as an "amplifying or recording device." *Id.*

Intentionally Record. Like her Section 631 claim, Plaintiff's Section 632 claim fails because her Complaint fails to allege that LinkedIn acted with "intent." (*See generally* Compl. ¶¶ 71-81.) Further, her only allegations regarding LinkedIn's state of mind merely parrot Section 631's elements. (*Id.* ¶¶ 67-68.) These allegations are insufficient under the statute, which requires that she allege "specific factual circumstances that make plausible [LinkedIn's] intent to record a confidential communication." *Vartanian v. VW Credit, Inc.*, 2012 WL 12326334, at *2 (C.D. Cal. Feb. 22, 2012) (finding allegation that Defendant "had a policy or practice of recording telephone

conversations" too conclusory to plead intent). Indeed, California courts have long held that Section 632(a)'s intent requirement is satisfied only if "the person using the recording equipment [did] so with the ***purpose*** *or* ***desire*** of recording a confidential conversation, or with the ***knowledge to a substantial certainty*** that his use of the equipment will result in the recordation of a confidential conversation." *People v. Super. Ct. (Smith)*, 70 Cal. 2d 123, 134 (1969) (emphases added). It is not enough to intend to use a recording device; instead, a defendant must ***intend to use it for an impermissible purpose***. This rule "provides effective protection against 'eavesdroppers' without penalizing the innocent use of recording equipment." *Id.* Plaintiff's perfunctory pleading, coupled with LinkedIn's policies specifically prohibiting advertising customers from sending sensitive information via the Insight Tag, belies any plausible inference of intent.

Device. Plaintiff's Section 632 claim also fails because she does not plead that the Insight Tag is an "amplifying or recording ***device***." Cal. Penal Code § 632(a). Plaintiff alleges that the tag "is a JavaScript-based code which allows for the installation of its software." (Compl. ¶ 25.) Numerous courts interpreting CIPA recognize that software is not a "device," and have dismissed CIPA claims challenging software. *A.S. v. SelectQuote Ins. Servs.*, 2024 WL 3881850, at *11 (S.D. Cal. Aug. 19, 2024) (dismissing Section 632 claim based on recording by software); *Doe v. Microsoft Corp.*, 2023 WL 8780879, at *8 (W.D. Wash. Dec. 19, 2023) (holding same) ("Because software does not constitute a 'device' under the CIPA, Plaintiff's § 632 claim against Microsoft is deficient."); *Moreno v. S.F. Bay Area Rapid Transit Dist.*, 2017 WL 6387764, at *5 (N.D. Cal. Dec. 14, 2017) (holding "device" does not apply to software under CIPA § 637.7); *In re Google Location Hist. Litig.*, 428 F. Supp. 3d 185, 193 (N.D. Cal. 2019) (holding same). This approach is consistent both with rules of statutory construction and CIPA's legislative history.

In interpreting California law, courts look to the "actual words of the statute" and "giv[e] them a plain and commonsense meaning." *In re Google Location Hist. Litig.*, 428 F. Supp. 3d at 193 (quoting *Cal. Teachers Ass'n v. Governing Bd. of Rialto Unified Sch. Dist.*, 14 Cal. 4th 627 (1997)). In *Moreno*, the Court interpreted a different provision of CIPA and observed that a device is generally understood as a "thing," "a piece of mechanical or electronic equipment," or "a piece of equipment or a mechanism designed to serve a special purpose or perform a special function."

2017 WL 6387764, at *5. It then concluded that because the term "device" refers to a physical object, it did not apply to the software at issue. *Id.*; *see also In re Google Location Hist. Litig.*, 428 F. Supp. 3d at 193 (holding same). Legislative history is consistent with this interpretation. The legislature chose to limit Section 632 to electronic "devices," and although the statute was modified in 2017 by AB 1671, those revisions did nothing to modify the statute to address software.

LinkedIn acknowledges that a handful of courts in this district have allowed plaintiffs to allege that software is a "device" for purposes of section 632. In *Doe v. Meta Platforms* and *Yockey*, the Court found that software was a device for purposes of § 632 based on cases interpreting the term in the federal Wiretap Act. *Doe v. Meta Platforms, Inc.* 690 F. Supp. 3d 1064, 1080 (N.D. Cal. 2023), *motion to certify appeal denied*, 2024 WL 4375776 (N.D. Cal. Oct. 2, 2024); *Yockey*, 2024 WL 3875785, at *7. But neither of those courts considered legislative history or the plain language of the statute, and the federal Wiretap Act cases on which those courts relied invoked the definition of "device" in the Wiretap Act, which has no application here. *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1084 (N.D. Cal. 2015) (construing language in the definition of "device" under Wiretap Act). Instead, this Court should adopt the same reasoning it applied in *In re Google Location History Litig*, in which it dismissed a claim under a different provision of CIPA, observing that "Software like Google Maps, Chrome, etc. are not 'devices' within the meaning of CIPA because they are not 'equipment.'" *In re Google Location Hist. Litig.*, 428 F. Supp. 3d at 193 (citation omitted). The same is true here—Insight Tag is no closer to being a device than Google Maps is.

Confidential. Lastly, Plaintiff does not plausibly allege that her online communications with CityMD were "confidential" within the meaning of the statute. "A communication is confidential under Section 632 if a party 'has an objectively reasonable expectation that the conversation is not being overheard or recorded.'" *Swarts*, 689 F. Supp. 3d at 746 (citation omitted). Because online "communications can easily be shared by, for instance, the recipient(s) of the communications," "California appeals courts have generally found that Internet-based communications are not 'confidential' within the meaning of [S]ection 632[.]" *Id.* at 746-47 (quoting *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014)) (collecting cases). Indeed, there is a "presumption' that such communications do not give rise to the requisite

expectation." *Id.* at 747 (quoting *Revitch v. New Moosejaw, Inc.*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019)). That presumption should apply here, and Plaintiff's claim should be dismissed for this reason as well.

D. Plaintiff's Section 631 and 632 Claims Also Fail Because She Has Not Alleged Interception of "Content."

To state a valid claim, Sections 631 and 632 of CIPA both require that Plaintiff plausibly allege that LinkedIn unlawfully intercepted "communications." §§ 631(a), 632. Here, Plaintiff alleges that LinkedIn receives "information including the patient's appointment time, who the appointment was for," general reasons from a pre-determined list as to "why they were booking the appointment" and their "gender." (Compl. ¶ 41.) Such information is not a "communication." The Massachusetts Supreme Court recently confronted this exact issue in a similar challenge to the use of MetaPixel and Google Analytics on hospital websites. *Vita v. New England Baptist Hosp.*, 243 N.E.3d 1185 (Mass. 2024). There, hospital websites used pixel technology that purportedly transmitted, *inter alia*, the URL of the webpages visited, the titles of webpages visited, and "the filtering criteria selected . . . including specialty, location, gender, and language." *Id.* 1190-91. In construing Massachusetts' law's statutory text, the court observed that the statute did not specifically define "communication." *Id.* at 1188. It further noted that "it does seem clear that the plain meaning of 'communication' includes messages and conversations between people" and held that Plaintiffs' complaints "do not allege communications between people in this commonsense way." *Id.* at 1196-97. After surveying legislative history and case law, the Court determined "the rule of lenity must apply, thereby entitling the defendants to 'the benefit of any rational doubt' in the construction of the statute.'" *Id.* at 1195-96 (citation omitted). It then dismissed the wiretap claims.

Vita's reasoning is relevant here. Like the Massachusetts Wiretap law, CIPA does not define "communication." Further, Plaintiff does not plausibly allege that the browsing information identified in her pleading is akin to a communication in accordance with that term's plain meaning. *Campbell v. Allied Van Lines Inc.*, 410 F.3d 618, 620–21 (9th Cir. 2005) ("Under the 'plain meaning' rule, [w]here the language [of a statute] is plain and admits of no more than one meaning the duty of interpretation does not arise[.]") (citation omitted). Accordingly, the Court should

dismiss each of her CIPA claims for this independent reason.

E. Plaintiff Fails to State a Claim for Invasion of Privacy Under the California Constitution.

The California Constitution, Article I, Section 1 "set[s] a high bar for an invasion of privacy claim." *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (Koh, J.). To state a claim for invasion of privacy, a plaintiff must allege (1) a legally protected privacy interest, (2) a reasonable expectation of privacy under the circumstances, and (3) highly offensive conduct by the defendant that amounts to a serious invasion of the protected privacy interest. *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35–37 (1994). Since these elements overlap with the elements of a common law claim for intrusion upon seclusion, case law analyzing these causes of action is often considered interchangeably. *See, e.g.*, *Hammerling v. Google LLC*, 2022 WL 17365255, at *8 (N.D. Cal. Dec. 1, 2022) (analyzing the tests together).

Where, as here, the invasion of privacy claim shares a factual basis with a defective wiretapping claim (*see, e.g.*, Compl. ¶¶ 82-88), it should likewise be dismissed. *Graham*, 533 F. Supp. 3d at 836 ("Because there was no plausible wiretapping by FullStory, the plaintiffs did not plausibly plead that they possess a legally protected privacy interest."); *Yale v. Clicktale, Inc.*, 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021) (same). But even if the Court considered the Plaintiff's constitutional claim on its own merit, Plaintiff's allegations fall short of clearing the California Constitution's "high bar" for stating a claim.

1. Plaintiff Fails to Allege Any Protected Privacy Interest.

"Just as the right to privacy is not absolute, privacy interests do not encompass all conceivable assertions of individual rights." *Hill*, 7 Cal. 4th at 35. Legally recognized privacy interests are generally categorized into "two classes: (1) interests in precluding the dissemination or misuse of sensitive and confidential information ('informational privacy'); and (2) interests in making intimate personal decisions or conducting personal activities without . . . intrusion . . . ('autonomy privacy')." *Id*. Plaintiff alleges neither.

a. Plaintiff Fails to Allege an Informational Privacy Interest.

"[C]ourts hearing information privacy cases focus ***both*** on the nature of the stored

information and the way it is used." *Jones v. Tonal Sys., Inc.*, 2024 WL 4357558, at *13 (S.D. Cal. Sept. 30, 2024). First, the "primary objective" of informational privacy is "to regulate [] unnecessary collection ***and improper use*** of [personal] information for dissemination." *Dep't of Fair Employment & Housing v. Super. Ct.*, 99 Cal. App. 4th 896, 904 (2002) (emphasis added). No informational privacy interest is implicated here because Plaintiff fails to allege, as she must, that LinkedIn disseminated or misused her information, *See, e.g.*, *id.*

Plaintiff also fails to allege that sensitive and confidential information is at issue. *Hill*, 7 Cal. 4th at 35. Most personal information is not constitutionally protected. *See Cabral v. Supple, LLC*, 2012 WL 12895825, at *3 (C.D. Cal. Oct. 3, 2012). Protected information must be "private," such that "well-established social norms recognize" that dissemination or misuse may cause "unjustified embarrassment or indignity." *Hill*, 7 Cal. 4th at 35. Plaintiff attempts to shoehorn the information at issue into the category of "sensitive, confidential communications and protected health information." (Compl. ¶ 85.) "Medical patients' privacy interests . . . include descriptions of symptoms, family history, diagnoses, test results, and other intimate details concerning treatment," but Plaintiff alleges none of these, nor equivalently private information. *St. Aubin*, 2024 WL 4369675, at *12 (citation omitted). Again, the challenged information is neither sensitive nor private, and is instead merely (1) gender plus logistical information limited to (2) unremarkable urgent care appointment information (location and time) and (3) the appropriate billing-related category ("Regular urgent care," "Employer Referred (Occupational Medicine)," "Work Related Injury," "Motor Vehicle Accident," or "[Department of Transportation] Physical.") (Compl. ¶¶ 39, 41.) ***None*** of this even approaches sufficient sensitivity. *See, e.g.*, *Pettus v. Cole*, 49 Cal. App. 4th 402, 441 (1996) (finding reports disclosing a patient's private anxieties about his rash medication together with his sleep patterns, sex drive, hostile feelings toward coworkers, suicidal ideation, smoking and drinking habits, comprehensive social history, and highly emotional behaviors as reported by physicians to be "the type of 'sensitive personal information' the California voters had in mind").

b. Plaintiff Fails to Allege an Autonomy Privacy Interest.

California courts have recognized an autonomy privacy interest only where invasions into

physical, bodily choices are implicated. Plaintiff pleads no facts suggesting bodily autonomy is at issue, and courts have not found "cause to extend the bodily autonomy line of cases to data autonomy." *In re Google Location History Litig.*, 428 F. Supp. 3d at 198 (collecting cases); *see In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1039 (N.D. Cal. 2014) (noting California Courts' limitation of autonomy privacy to "cases alleging *bodily* autonomy")). Fact patterns raising the issue of autonomy privacy involve physical, real-world invasions of privacy, such as constraints on women's decisions about bearing children or mandatory drug testing through forced urine samples. *Comm. to Def. Reprod. Rights v. Myers*, 29 Cal. 3d 252, 275 (1981) (noting constitutional right of privacy in women's "personal bodily autonomy"); *Smith v. Fresno Irrigation Dist.*, 84 Cal. App. 4th 147, 161-62(1999) (discussing autonomy privacy in the context of drug testing through use of a urine sample). Plaintiff's vague assertions that she has "an interest in . . . making personal decisions and/or conducting personal activities without observation," (Compl. ¶ 85), allege no physical intrusion compromising her bodily autonomy and she therefore alleges no autonomy privacy interest.

2. Plaintiff Fails to Allege a Reasonable Expectation of Privacy in Her Online Commercial Activity.

Plaintiff's constitutional claim fails for the additional reason that her expectation of privacy was not reasonable under the circumstances. In general, a "reasonable expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms." *Hill*, 7 Cal. 4th at 37. In cases challenging the data collection practices of corporate actors, courts consider factors including "the amount of data collected, the sensitivity of data collected, the manner of data collection, and the defendant's representations to its customers." *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1088 (N.D. Cal. 2022). Here, the amount of data allegedly collected was minimal, confined to particular interactions on a particular portion of a single website, and Plaintiff inadequately alleges that such data were sensitive. *Supra* Sec. II.C.1.b; *see, e.g.*, *D'Angelo v. FCA US, LLC*, 726 F. Supp. 3d 1179, 1205 (S.D. Cal. 2024) ("[C]ourts are more reluctant to find a reasonable expectation of privacy when the data collected is not sensitive.").

Plaintiff fails to allege a reasonable expectation of privacy because nothing in her pleading

demonstrates that expectation was ***reasonable*** under the circumstances. Plaintiff concedes that she voluntarily visited CityMD's website and transmitted limited logistical information to CityMD, and nowhere plausibly alleges that such transmissions should remain private from ***CityMD or its agents***. Virtually all consumer-facing websites track the conduct of web visitors. *See, e.g.*, *Thomas v. Papa Johns Int'l, Inc*., 2024 WL 2060140, at *3 (S.D. Cal. May 8, 2024) (noting that the proliferation of litigation in this area "suggest[s] Defendant is not alone in this practice," and finding that this is "a factor to consider"). Generally speaking, "consumers do not have a reasonable expectation of privacy over their activity" on publicly accessible websites, because we "understand that what we do on the Internet is not completely private." *Id.* at *2; *see D'Angelo v. Penny OpCo, LLC*, 2023 WL 7006793, at *10-11 (S.D. Cal. Oct. 24, 2023) (no reasonable expectation of privacy on public website); *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 524-25 (C.D. Cal. 2021) (same); *Saeedy v. Microsoft Corp.*, 2023 WL 8828852, at *4 (W.D. Wash. Dec. 21, 2023) (same). Given that the challenged practices are nearly universal on consumer-facing websites, no user can reasonably expect that the web pages she visits, or the information she provides on such a website, are completely private.

Finally, Courts are similarly skeptical where "Plaintiffs do not allege that Defendant set out an expectation that it would not collect" the challenged data. *D'Angelo*, 726 F. Supp. 3d at 1205. Here, Plaintiff herself alleges that LinkedIn's Privacy Policy clearly discloses that it "use[s] cookies and similar technologies (e.g., pixels and ad tags) to collect data (e.g., device IDs) to recognize you and your device(s) on, off and across different services and devices where you have engaged with our Services,'" and "'allow[s] some others to use cookies as described in our Cookie Policy.'" (Compl ¶ 34 (quoting Privacy Policy, LinkedIn, https://www.linkedin.com/legal/privacy-policy (Sept 18, 2024)).) LinkedIn also explicitly tells users "[w]e receive information about your visits and interaction with services provided by others when you visit others' services that include some of our ads, cookies or similar technologies." (Reddy Decl. Ex. D, LinkedIn Privacy Policy at § 1.8.) All the challenged data here falls under these two disclosures. Thus, because LinkedIn disclosed precisely the data practices Plaintiff challenges, she fails to allege any reasonable expectation of

privacy. *Hill*, 7 Cal. 4th at 26; *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1037–38.[3]

3. The Routine Commercial Behavior Alleged Is Not Highly Offensive as a Matter of Law.

"Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *Hill*, 7 Cal. 4th at 37. A "highly offensive" intrusion must constitute an "egregious breach of the social norms underlying the privacy right." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (quoting *Hill*, 7 Cal. 4th at 26, 37). This high standard requires more than mere "disclosure of personal information," *Low*, 900 F. Supp. 2d at 1025, and indeed, more than mere "private medical information." *Ojeda v. Kaiser Permanente Int'l, Inc.*, 2022 WL 18228249, at *6 (C.D. Cal. Nov. 29, 2022) (disclosure of Covid vaccination status, though politically fraught, not highly offensive on facts alleged). Instead, courts undertake a holistic consideration of "factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, [and] the intruder's motives and objectives[.]" *See, e.g.*, *Cousin v. Sharp Healthcare*, 681 F. Supp. 3d 1117, 1126 (S.D. Cal. 2023); *Hammerling*, 2022 WL 17365255, at *8. Each favors dismissal with prejudice.

First, Plaintiff fails to plead any risk of "serious harm," much less with the requisite specificity as to, for example, "the form and extent of the distress and alienation suffered," such as being "singled out" for coworkers' approbation. *Ojeda*, 2022 WL 18228249, at *7. Because Plaintiff merely offers vague claims of unspecified "economic injury" and "breach of Plaintiff's privacy" (Compl. ¶¶ 6, 53), on the facts alleged—limited disclosure of information to a single party—this Court should conclude that she ***cannot*** satisfy the pleading standard.

Second, Plaintiff's allegations that LinkedIn received information revealing her selections in CityMD location, appointment time, and billing category (Compl. ¶¶ 8, 39, 41) insufficiently allege "***what***, if any, medical information or medical records were transmitted or disclosed." *B.K.*

[3] While Plaintiff alleges that she did not consent to purported interception, (Compl. ¶ 46), "allegations that a plaintiff did not consent to data collection practices, without more, does not support a reasonable expectation of privacy." *D'Angelo*, 726 F. Supp. 3d at 1206.

v. Eisenhower Med. Ctr., 721 F. Supp. 3d 1056, 1064 (C.D. Cal. Feb. 29, 2024) (emphasis added). Courts have dismissed invasion of privacy claims in evaluating allegations far more detailed than what Plaintiff here alleges. For example, in *B.K. v. Eisenhower Medical Center*, the plaintiff alleged that "[w]hile using Eisenhower Health's digital services, Plaintiff communicated and received information regarding her appointments, treatments, medications, and clinical information, including her surgeries, lab work, and scans" and that the Meta Pixel caused the information to be "intercepted, viewed analyzed [sic], and used by unauthorized third parties." Compl. ¶¶ 174-176, *B.K. v. Eisenhower Medical Center*, No. 5:23-cv-2092 (C.D. Cal. Oct. 12, 2023), ECF No. 1. The court held that these allegations were ***insufficiently specific*** to survive dismissal. By contrast, the plaintiff in *St. Aubin* survived dismissal because she alleged that "the transmitted URLs contain information regarding the ***specific symptoms, physical condition, or course of treatment*** of an individual." 2024 WL 4369675, at *12 (N.D. Cal. Oct. 1, 2024) (emphasis added). In allowing the claim to proceed, the *St. Aubin* court distinguished the defendant's cited cases on the basis that "they [did] not involve information that revealed ***the nature of a patient's treatment***." *Id.* at *10 (emphasis added). Because Plaintiff likewise fails to allege that LinkedIn received any information revealing a specific medication condition, history, or treatment, she has not alleged disclosure of any "medical information" to which courts have applied constitutional privacy protections.

Third, Plaintiff cannot rely on her generic allegations that "LinkedIn utilized Plaintiff's . . . information for its own purposes, including for targeted advertising" (Compl. ¶ 81), to evidence some incriminating motive. *Hammerling* is again instructive. Noting that "[t]he provision of new, improved, and more personalized services is . . . largely indistinguishable from, [defendant] Google's 'commercial purposes,'" the Court was "unpersuaded that Plaintiffs' alleged motive for Google's data collection—that 'Google was using the data for its own purposes' . . . —alter[ed] this conclusion." *Hammerling*, 2022 WL 17365255, at *9 n.13. Further, Plaintiff does not plead any facts suggesting LinkedIn's alleged receipt of her information was "intentional, punitive, [or] reckless" rather than "inadvertent." *Ojeda*, 2022 WL 17227249, at *7. "[N]o cause of action will lie for accidental, misguided, or excusable acts of overstepping upon legitimate privacy rights." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 295 (2009). Even where "privacy

damage . . . is serious," a plaintiff must allege "***intentional***, egregious privacy invasion[.]" *Razuki v. Caliber Home Loans, Inc.*, 2018 WL 2761818, at *2 (S.D. Cal. June 7, 2018). By contrast, courts have held that allegations of "accidental" conduct "of the kind that is inevitable when human beings process large amounts of information" are "not necessarily sufficient to sustain a claim under article I, § 1" of the California Constitution. *Doe v. Beard*, 63 F. Supp. 3d 1159, 1169 (C.D. Cal. 2014).

Instead of suggesting any culpable motive, this limited collection of logistical information alleged is "routine commercial behavior," which courts consistently find is not highly offensive. *Fogelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011). LinkedIn's Insight Tag is a ubiquitous commercial technology, and this Court should easily find that use of such technology is routine commercial behavior rather than any highly offensive practice. *Fogelstrom* is highly instructive on this point: There, as here, the challenged practice included alleged nonconsensual obtainment of the plaintiff's personal information, which was used to serve advertisements to him. *Id*. The court in that case found that "the conduct of which plaintiff complains does not constitute a 'serious' invasion of privacy." *Id.* Similarly, in *Yunker v. Pandora Media, Inc.*, the court found allegations that defendant "Pandora obtained the [plaintiff's PII] and provided that information to advertising libraries for marketing purposes" to be "similar to the allegations in . . . *Fogelstrom*[.]" 2013 WL 1282980, at *15 (N.D. Cal. Mar. 26, 2013) (finding plaintiff's allegations insufficient to show highly offensive conduct). This Court should reach the same conclusion.

Courts find allegations of a highly offensive intrusion sufficient only where there are far more extreme, pervasive intrusions than limited collection of generic consumer selections on certain pages of a single website. *See, e.g.*, *Goodman v. HTC Am., Inc.*, 2012 WL 2412070, at *15 (W.D. Wash. June 26, 2012) (finding allegations "that Defendants engaged in the continuous tracking of their location and movements" plausibly highly offensive because "GPS monitoring generates a precise, comprehensive record . . . that reflects a wealth of detail about . . . familial, political, professional, religious, and sexual associations"); *In re Google Location History Litig.* 514 F. Supp. 3d 1147, 1158 (N.D. Cal. 2021) (same where plaintiffs did not "allege that Google only collected information at discrete, intuitive times, but rather, they specifically allege that Google collected location information constantly"). Such facts are worlds away from this case.

Dated: January 27, 2024

COOLEY LLP
By: */s/ Jeffrey M. Gutkin*
Jeffrey M. Gutkin
Attorney for Defendant
LINKEDIN CORPORATION

313043823